Remarks

The various parts of the Office Action (and other matters, if any) are discussed below under appropriate headings.

Claims 49, 50 and 73 have been cancelled without prejudice.

Claim Rejections - 35 USC § 102 and § 103

Claims 1, 3-48, 51, 61-63, 65-69 and 74 have been rejected under 35 U.S.C. § 102(e) as being clearly anticipated by U.S. Patent No. 5,754,654 to Hiroya et al. ("Hiroya") or by U.S. Patent No. 5,898,154 to Rosen ("Rosen"). The undersigned respectfully submits, however, that the claims are not anticipated by either Hiroya or Rosen.

The Examiner's detailed comments in the Office Action are appreciated. Before turning to those comments and the rejections, the undersigned asks the Examiner to consider the following remarks concerning the claimed invention. As is set out on page 1 of the application, the claimed invention relates to electronic transactions or transfers using an electronic representation of a commodity, such as money in the form of U.S. dollars or British pounds, for example. The claimed invention is especially suitable for use in financial transactions and is especially suitable for use over a public communication network (e.g., the internet). However, there are a number of concerns particular to such electronic money systems, including those given over pages 1 and 2 of the application. These concerns include:

1. SECURITY- It is desirable to prevent fraudulent interference with transactions involving electronic money as well as to prevent the same electronic money from being spent more than once.

2. ANONYMITY- For a user of an electronic money system, it may be desirable for the user's identity to remain confidential.

The claimed invention addresses these security and anonymity concerns by providing the "*value notes,*" as specified in each of the independent claims 1, 13, 28, 61, 63 and 65.

Claim 1

Claim 1, for example, recites a method of providing a value note comprising the following steps:

> providing first information representative of a bearer's public key information, or from which a bearer's public key information can be verified;
>
> providing second information representative of a commodity represented by the value note; and
>
> calculating third information representative of an issuer's signature dependent on the first and second information and verifiable by means of an issuer's public key information.

The Examiner's attention is drawn to the following two features of claim 1.

1. The first information is representative of a **bearer's** public key information, or is such that a **bearer's** public key information can be verified from it. It is extremely important to understand that the bearer is the bearer of the note (that is to say **the user or redeemer** of the note) **in contrast to the issuer of a note**, for example an issuing bank. This is clear from the specification (pages 1 to 10), in particular page 4, lines 8 to 12, and page 6, lines 8 to 18.

2. The step of calculating third information representative of an issuer's signature is dependent on the first and second information. As appreciated by the Examiner in paragraph 8 of the final Office Action (Paper No. 17), the first and second information is signed with a single signature.

Advantageously, the first feature (the first information representative of a bearer's public key information) enables the bearer to remain anonymous. "*By using a public key in this way, the bearer can remain anonymous since the public key information does not have to identify the bearer.*" (Specification, page 6, lines 13 and 14.)

In addition to this first feature, the second feature (the step of calculating third information representative of an issuer's signature dependent on the first and second information) affords security.

> *The value note is secure because the issuer's signature protects the public key information and the commodity information to prevent it from being altered. Should either or both of these items of information be altered, then the issuer's signature will no longer match the altered information, and this is easily verifiable by the bearer without having to contact the issuer.*

(Specification, page 5, lines 17-20.)

In contrast, the applied prior art, Hiroya and Rosen, fails to address the security and anonymity concerns or considerations provided by these features of the claimed invention. Consequently, the skilled person in the art is unlikely to consider Hiroya or Rosen when addressing these concerns. Furthermore, even if the skilled person were to consider addressing these considerations with reference to the applied prior art, nothing has been found in either reference to suggest the method of claim 1. The method of claim 1 is simply not taught or suggested by the applied prior art. In addition, modifying Hiroya, at least, to arrive at the method of claim 1 is technically impossible (as is discussed in detail below). The claimed arrangement therefore provides significant advantages and clearly defines over the applied prior art.

Moreover, the second feature of the claimed arrangement described above, in contrast to the Examiner's assertions in paragraph 8 of the Office Action (Paper No. 17), is far from *"a clear and understandable design choice."* Firstly, careful consideration of Hiroya shows that it is technically impossible to modify the teaching of Hiroya to arrive at the claimed method. Secondly, as ascertained by the Examiner, the increased security provided by using a single signature rather than using more than one signature is *"counterintuitive,"* which could be re-phrased as *"surprising"* or *"not suggested,"* rather than being *"a clear and understandable design choice,"* and clearly indicates the patentable merit of method claim 1 over Hiroya.

Hiroya

In paragraph 12 of the final Office Action, the Examiner rejected claim 1 as anticipated by Hiroya because:

> Hiroya et al. teach an electronic ticket vending system such that Applicant's value note reads on the electronic ticket storage device, applicants first information reads on PTi, Applicant's second information reads on the ticket information, 610, and Applicant's step of calculating third information (RSA type signature-asymmetric encryption algorithm) leads on to Stk and column 15, lines 38-44.

Paper No. 17, page 5. However, Hiroya fails to teach or suggest the step of calculating third information representative of an issuer's signature dependent on the first and second information, as set forth in claim 1, and also fails to disclose first information representative of a bearer's public key information, also set forth in claim 1. Thus, the teaching of Hiroya is quite different from the method of claim 1.

Hiroya relates to an electronic ticket vending system and a method of using electronic money for purchasing tickets (see Hiroya, *"Field of Invention,"* column 1, lines 6-14). This is in contrast to the field of the present application which relates to electronic transactions in general, rather than one particular type of transaction as in Hiroya.

The Hiroya system involves a ticket purchaser purchasing a ticket by operating a terminal device that communicates with an electronic ticket vending and refunding device (see Hiroya, column 6, line 62 to column 8, line 22 and Figure 1). The electronic ticket vending and refunding device issues an electronic ticket and the terminal device stores the ticket in an electronic ticket storage device. The same communication procedure (using an asymmetric encryption algorithm) is used for the transmission of the electronic ticket as for the transmission of the electronic money (see Hiroya, column 8, lines 16-21).

This communication procedure is described in Hiroya from column 13, line 61 to column 14, line 46, and includes using an "electronic purse." Each electronic purse retains Pg (a global public key), SLi (a local public key) and PLi*Sg (PLi encrypted by a global secret key, Sg). Sg itself is not retained in the electronic purse. The *"i"* in the naming system used in Hiroya is replaced by *"r"* for the receiving side and *"s"* for the sending side.

The electronic purse on the receiving side sends PLr*Sg, receiving side's public local key encrypted by the global secret key, and R*SLr, the message encrypted by the receiving side's secret local key, to the electronic purse on the sending side. R is the message (the financial transaction, for example). To read the message the sending side firstly uses Pg, the global public key, to decrypt PLr*Sg and obtain PLr, and then secondly uses the so-obtained PLr to decrypt R*SLr to obtain R.

The whole Hiroya system relies on this two-step type of encryption/decryption where PLr*Sg is decrypted to obtain PLr to then decrypt the second pair of the communication. The receiving side only retains Pg, SLi, PLi and PLi*Sg. Importantly, the receiving side does not retain Sg itself. It is therefore technically impossible for the Hiroya system to send R*Sg (i.e., a message signed by a single signature as provided by the claimed invention and described by the Examiner as *"a clear and understandable design choice"*) because the receiving side retains R but not Sg. Sg, the global secret key, is managed under strict management of a generalizing manager (see Hiroya, column 16, lines 49-51). Sg is simply not available to the receiving side, and thus modifying Hiroya to arrive at the method of claim 1 is technically impossible.

Hiroya also reverses the usual "public key" and "secret key" terminology. The undersigned respectfully submits a copy of Chapter 19 from Applied Cryptography, 2nd ed., written by Bruce Schneier. Chapter 19 is entitled "Public-Key Algorithms" and discusses the RSA algorithm. (see Applied Cryptography, p. 466.) The author describes how to compute the public and private key for a given user. (see Applied Crytography, p. 467.) The secret key is designated *d* (decryption key) and the public key is designated *e* (encryption key). The author notes that *e* is published while *d* is kept secret. (see Applied Cryptography, p. 468.) Schneier also makes clear that the public key is used for encryption and the secret key is used for decryption. (see Applied Cryptography, p. 467).

In contrast, Hiroya states that an asymmetric encryption algorithm represented by the RSA system is used by the electronic ticket storage device and the electronic ticket vending and refunding device. (see Hiroya, column 13, line 66 to column 14, line 1). Contrary to the general understanding of the RSA algorithm for encryption, however, Hiroya uses the secret key to encrypt data and the public key to decrypt data. (see Hiroya, column 14, lines 4-18). Specifically, Hiroya has a sender perform the operation of PLi * Sg, which is the local public key encrypted by a global secret key, and sends this data to a receiver. The receiver then obtains Sg, the global secret key, by decrypting the data with Slr, the local secret key. (see Hiroya, column 14 lines 4-18).

Hiroya reverses the usual meanings for the terms "public key" and "secret key." Where the published RSA algorithm encrypts data using a public key, Hiroya encrypts data with the secret key; where the published RSA algorithm decrypts data with a secret key, the Hiroya patent decrypts data with a public key. By reversing the meanings of the terms "public key" and "secret key," Hiroya teaches away from the standard use of the RSA algorithm, and therefore, would not suggest to a person with ordinary skill in the art that Hiroya should be modified to reach Applicant's method.

Consequently, feature 2 (the step of calculating third information representative of an issuer's signature dependent on first and second information) also is not taught or suggested by Hiroya. Unlike the claimed invention, in Hiroya the signature generation is calculated by the issuer without regard to first information sent by the bearer.

To send a message from the bearer (i.e., the electronic ticket storage device) to the issuer (i.e., the electronic ticket vending and refunding device), Hiroya asks the bearer to send PT12 * STg + R * ST12 to the issuer, representing the public key of the electronic ticket storage device encrypted by the global secret key, and the message encrypted by the secret key of the electronic ticket storage device. (see Hiroya, column 17, line 9). In this example, PT12 * STg represents first information sent by the bearer. The issuer then obtains PT12 by decrypting it with the global public key PTg and obtains R by decrypting R * ST12 with PT12. (see Hiroya, column 17, lines 12-15). Before sending an encrypted message back to the bearer, the issuer generates an electronic signature for inclusion in the encrypted message. The electronic signature is created by encrypting part of the message R with the issuer's local secret key ST11 (see Hiroya column 15, lines 41-48; column 16 lines 61-65; and column 17, lines 15-19).

The system described in Hiroya clearly does not rely on first information sent by the bearer to generate the electronic signature. In claim 1, Applicant's third limitation is that the electronic signature's calculation is dependent on "the first and second information" where the first information is "representative of a bearer's public key information." But Hiroya calculates the electronic signature using the issuer's local secret key and not the bearer's public key. Not only is the key's source different from Applicant's, but the key itself is different. Hiroya uses a method very different from the method claimed by Applicant. This in itself means claim 1 is patentably distinguished over Hiroya.

However, claim 1 is further distinguished by feature 1 (the first information representative of a bearer's public key information). The Examiner has cited Hiroya, column 15, lines 38-44 (see paragraph 12 of the Office Action, Paper No. 17) in this regard. However, this section of Hiroya only discloses T*STk, i.e., the ticket information T encrypted by STk, the ticket publisher's secret key. Importantly, it should be noted that in the cited passage STk and PTk are a key pair belonging to the same entity and not one belonging to an issuer and the other belonging to a bearer as required by the claim.

Assuming the Examiner is equating Hiroya's publisher to the issuer of claim 1, which appears to be the case, then there is no disclosure of the bearer's public key information in this cited passage. (Conversely, if the Examiner is equating Hiroya's publisher to the bearer of claim 1 then there is no disclosure of calculating third information representative of an issuer's signature). Thus, the method of claim 1 is further patentably distinguished over Hiroya by feature 1 (the first information representative of a bearer's public key).

Withdrawal of the rejection is respectfully requested.

Rosen

The method of claim 1 is distinguished over Rosen for much the same reasons as it distinguishes over Hiroya. The Examiner has rejected claim 1 because:

> Rosen teaches an electronic monetary system such that Applicant's value note reads on element 11, Applicant's bearer's public key information (first information) reads on the identifier for money generator module, element 6. Applicant's information representative of a commodity (second information) reads on the type of note (credit or currency), Applicant's issuer's signature and issuer's public key information reads on the issuing bank's identifier and column 14, lines 6-14, applicants redemption instruction information reads on column 19, lines 30-65 (body group of data fields) and Applicant's bearer's signature reads on the digital signature of the Money Generator module, element 6 and columns 19 and 20, lines 54-67 and lines 1-4, respectively.

Paper No. 17, page 9.

In Rosen (see Rosen, column 6, lines 45-47), element 11 notes are first generated by the money generator module. These notes are then transferred by a teller money module 5 to a subscriber utilizing a transaction money module 4. The money generator module 6 creates and digitally signs electronic objects having economic value - either currency or credit notes - that are sent to the transaction money modules 4 in the form of electronic notes. The electronic notes are the equivalent of bank notes (see Rosen, column 9, lines 11).

The Examiner's assertion that the first information reads on the identifier for the money generator module, element 6, is unfounded. This identifier is not representative of a bearer's public key information because the money generator module is controlled by the bank, not the bearer of the note.

Thus in Rosen, like Hiroya, only the currency or credit note is signed, i.e., the value information is signed (e.g., the second information of claim 1), but the first information representative of a <u>bearer's</u> public key information is not signed.

Like Hiroya, Rosen does not teach or suggest feature 1 (the first information representative of a bearer's public key information) or feature 2 (the calculating third information representative of an issuer's signature dependent on the first and second information) of the claimed invention. Further it is not clear what would motivate the skilled person to modify this teaching of Rosen, nor is it clear how such modification would arrive at the claimed method.

Withdrawal of the rejection is respectfully requested.

Allowable Subject Matter

The Examiner's indication that claims 52 and 53 include allowable subject matter is greatly appreciated. Claim 52 has been amended to independent form and thus should be allowable.

Conclusion

In view of the foregoing, request is made for timely issuance of a notice of allowance.

Respectfully submitted,

RENNER, OTTO, BOISSELLE & SKLAR, LLP

By Christopher B. Jacobs
Christopher B. Jacobs, Reg. No. 37,853

1621 Euclid Avenue
Nineteenth Floor
Cleveland, Ohio 44115
(216) 621-1113